METHOD FOR USE IN A NETWORK BASED SAFETY DATA STORAGE SYSTEM

Description

[0001] The present invention relates to the field of security for access and data storage on servers operating in free-access networks.

Background Information

[0002] There are a number of applications for the security and provision of data, for example, over the Internet, whose specific features are described below.

[0003] The application Cryptoheaven (see http://www.crytoheaven.com) is a Java application (applet/Java plug-in). Similarly to MS Explorer, the display is divided, on the left, into a directory tree (incl. the local computer) and a contact list. Settings can be made via the right mouse button/popup. A proprietary protocol via port 82 is used. Data compression is used. Files are signed and encrypted. Files can also be uploaded from the local file system using drag and drop (DnD). The sequence control substantially corresponds to that of MS Explorer. The encryption is done locally on the client computer. Directories can be created, deleted and renamed. Access to directories is enabled for "invited users". The invitation is made via e-mail by users who have subscribed to the system. The invited must give his/her consent. Authentication is via user ID and password. The system is available for the operating systems Windows/Unix and Linux.

[0004] Another typical application exists in bvPREMIERE, bvPRO, bvPLUS+ and big VAULT Enterprise (see http://www.bigvault.com). The applications are specifically for Windows and allow a drive to be mapped (created) in MS Explorer, which is controlled via the WEB. The transmission protocol for uploading and downloading files is html over an SSl connection. File encryption is done on the server. Access to directories and files is enabled using a visitor password. There is an in-tray for authorized users. It is possible to log in as a user or visitor. Passwords with a limited validity period are set up in the same manner as has been done, for example, in UNIX for many years.

[0005] A further application offering an online file service for uploading/downloading is GLOBEDESK (see http://www.globedesk.com). Uploading/downloading via the browser is done using html or ftp. The connection is secured by SSL. Encryption is done on the server. The names of the subscribers are listed in a directory. A click on a name establishes connection to the available directories. User identification is done using e-mail and name.

[0006] The examples given are characterized by the following features:

- Security is based on a model using user name and password. Once a user has authenticated with his/her name and the associated password, the system is available to the user always in the same manner.

- The data is stored in a file system, or such that the functionality of a file system is exactly emulated for the user (such as mailboxes in Webmail).

[0007] With respect to security and to the storage system, the known applications have the following disadvantages:

- A security model based on user name and password can only implement the states access authorization granted or access authorization revoked. Finer control, for example, using time limits or intervals to be observed for access, is not possible, nor is it possible to limit the number of simultaneously accessing users.

- The storage model used is characterized as a registry of created folders, in which files are stored regardless of their type, and retrieved again unchanged. A freely selected classification by content cannot be controlled by the system itself. It is completely impossible for a folder to become active itself and, for example, to make backup copies of stored files, to time-stamp the files, or to delete them after predetermined storage periods.

[0008] The object of the present invention is to provide a method for access and data storage in telecommunications networks which overcomes the disadvantages of the known applications and provides significantly increased security.

[0009] The method is characterized in that it allows dependencies, such as the whereabouts, access time, terminal attributes, quality of communication paths, authentication method, etc., to be taken into account for the access rights, and in that it allows a security configuration according to the locker principle to be emulated for the data storage. The security is further enhanced by carrying out the encryption and decryption of files on the local computer of the user and by using an additional second encryption algorithm on the server, said second encryption algorithm being unable to be influenced by the user.

[0010] The aim of the data transfer is to store data in memories of servers in order to restore the data to the local computer when needed, to have the data processed on a remote computer, or to make the data available to third parties or to the user himself/herself at a different location for a certain period of time. The conditions under which access is allowed must be able to be precisely controlled and maintained. The storage of files requires a classification system which should provide clarity for the retrieval of files and optimally support data security.

[0011] The requirements for precise access control and a classification system for the storage of the files featuring high security are optimally met by the data storage system of the present invention. The data storage system includes the server and its special program operating in a telecommunications network as well as the local computers integrated over the network. The program on the server uses a storage model in the form of a locker system. The locker system has a virtual character because, depending on the access rights, only the lockers and files the user is authorized to access are displayed to the user. No information is provided to the user when access is denied. Instead, the lockers, sub-locker, and files for which the user is not authorized are not displayed to the user.

[0012] In order to access the server and use the programs, an authorization is required, said authorization being granted by the server operator. An application for this is available, for example, upon written request or via the Internet. The application must include all information required for the issuance of a user certificate. The certificate contains, inter alia, the public key of the user. The user has a secret key for this public key. Preferably, the secret key and the certificate are stored on a smart card, because in this way a high level of protection is achieved for the secret key. If this option is chosen, the user is provided with a

second pair of keys to allow the user to use the system without the smart card, if required. In this second pair of keys, the secret key is protected by a password selected by the user.

[0013] In order to identify the user, personal data is entered into a database along with a copy of the certificate. The server accesses this information to be able authenticate users and to provide a user directory accessible by all users. In particular, each user has a unique system name, which may differ from his/her natural name.

[0014] During registration, the server operator creates a personal area of the DS for the user, said personal area being called the main folder (1) of the user. Operating systems and databases store data and their management information in different ways. Here, the known model of folders (also: directories) and files is used for purposes of description. A file (containing the data) is always contained in a folder, which is either the so-called root folder, or is itself contained in a folder. Thus, starting from this folder, the root folder is reached via a chain of higher-level folders. The names of the folders in this chain are strung together to form the so-called path of the file. A file is uniquely described by its name and path.

[0015] In the data storage system described herein, each folder contains a special file containing security and management information for the server (Table 1). In the following, a "locker" is taken to mean the unit including the folder and the special file.

[0016] The main locker (main folder) contains further lockers which are set up by the operator and distinguished by function. These lockers include, inter alia, personal lockers (2), provisioning lockers (3), receiving lockers (4), public lockers (5) for the user, and a system locker (6) which can only be accessed by the server. The locker type is specified in the associated special file.

[0017] A reference to a file contains at least the name of the file to which it refers.

[0018] Personal lockers contain only user-stored references to the files of the user; the transferred files themselves are stored by the server in the system folder. Provisioning lockers are used by the user to store therein the references to his/her files for other users. Receiving lockers contain references offered to the user by other users, and public lockers contain references to files offered to all users. The user is able to set up sub-lockers in each locker of

any of the types mentioned above, and to store references in these sub-lockers. Said sub-lockers may, in turn, contain other sub-lockers.

[0019] Access to the server is established from the local computer by connecting to the Internet address of the server. In this manner, the server obtains the Internet address of the local computer. As a rule, the network operator connecting the local computer to the Internet uniquely identifies the access point (ISDN or ADSL connection, GSM, GPRS, WLAN, UMTS). In order for the server to receive this information, a contract may be required to exist between the network operator and the operator of the data security system, and the network operator must provide the technical facilities.

[0020] The server sends a special program, the so-called client program, to the local computer. It is also possible to install a client program on the local computer and to make the connection from the local computer. The client program connects itself to some of the systems existing on the local computer, for example, a smart card reader, a fingerprint scanner, a face recognition system, a GPS module, or a system configured to determine (or to approximately determine) the geographic location.

[0021] The client program allows the user to use the functions made available to him/her on the server side, and to enter the data required for executing the programs, provided he/she can successfully authenticate to the server. Depending on the type of components present (card reader, biometric system), the client program offers the user different ways of authentication (name/password, PIN, smart card, smart card with biometry). The method chosen, the authentication result, and the geographic data (if available) are transmitted to the server. If the authentication fails, the server disconnects the connection, and the client program is terminated. If successful, the user can chose whether he/she wishes to act as a normal user (default condition) or as an administrator. In the second case, the client program may request a new, high-quality authentication, such as via smart card and biometry.

[0022] The period of time from the authentication to the termination of the client program is referred to as session. Successful authentication in particular causes the system name of the user to be associated with the session. This makes it possible to separate a great number of sessions running in parallel, and allows the server and client program to control the rights of user to execute applications. The information transmitted by the client program, such as type

of authentication (name/PW, smart card, ...) and geographic location, as well as the starting time known to the server, the current time, and the address (Internet address or network operator identification) of the local computer form also part of the session data and are stored by the server.

[0023] The client program displays to the user the contents of his/her main locker and local file system in the form of a folder tree as known from Microsoft Explorer; the operation also being similar to that of the Explorer. In each instance, the system displays only the lockers and references for which the user is authorized in the current session. Authorization is verified by the server by comparing the data contained in the special file to the session data.

[0024] The lockers are represented by a specific graphical symbol to distinguish them from ordinary folders. If the user has administrator rights, the locker symbols are given a special color.

[0025] The special file of a locker is at no time visible, nor is it possible to make it visible. If the user is the administrator, then, upon request, the client program displays to him/her the (user-) changeable content of special file, allowing him/her to change entries.

[0026] The system locker is at no time visible. This property cannot be changed either, because the user has no direct or indirect access to the special file of the system locker.

[0027] Storing a file located on the local computer into the personal locker of the user is a multi-step process, which is carried out by the user using a program having one component in the client program and one component on the server. The user interface of the client program allows the user to select the file to be stored by path and name and to specify the destination path in his/her personal locker. The server informs the client program of the destination locker requirements to be met by the files to be stored. These requirements include the maximum size, specific format (doc, pdf), or the existence of a signature of the data. If the requirements are met, the client program loads the data contained in the file and generates a random number, the so-called access key (8), with which the data is encrypted using a symmetric encryption method. Subsequently, this access key is encrypted with the public user key to form the encrypted access key (9), and the access key is destroyed. In this manner, it is

achieved that the encrypted content of the file can be decrypted only by the user who is able to recover the access key with the aid of his/her secret key.

[0028] The file name, file type, file size, encrypted data, and the encrypted access key are sent to the program portion on the server side along with further data required according to Table 2. The program portion on the server side encrypts the data a second time using a symmetric key of its own, so that even theft of the data, of the encrypted access key, or of the secret user key would not allow access to the data. Then, said program portion generates a system-wide unique file identifier, which is used as an internal name for the encrypted data. The encrypted data is stored under this name in the system locker. Then, a reference is created in the destination folder, said reference including the name of the file as the file name and containing the file identifier, the encrypted access key, and information about the file (size, type).

[0029] If the user, as the owner of a file, wants to offer this file to another user, he/she acts as an administrator and sets up a user locker (7) for the other user in a provisioning locker. For this purpose, the server offers the user, via the client program, a user directory which is in the manner of a telephone book and from which the user selects the desired user as the addressee. The user can also set up a personal locker for a group of users. The server enters this user or these users into the properties file as co-owners of the locker.

[0030] Via the user interface of the client program, the owner informs the server of the file to be offered and its destination (a sub-locker set up by the owner) within the user locker. The client program sends this information to the server. The server checks whether the properties of the destination locker permit the desired operation, after which it sends a copy of the reference to the file back to the client program along with the public key of the addressee. The client program extracts the encrypted access key from the reference, prompts the user to restore the access key using his/her secret key, and then encrypts it with the public key of the addressee to form a new encrypted access key. The access key is destroyed, the new encrypted access key is entered into the reference, and the reference is returned to the server which stores it in the destination locker. Then, a locker having the name of the owner is created in a receiving locker of the addressee.

[0031] Thus, the user now has a reference to the file along with a personal access key encrypted access key.

[0032] When the user opens a receiving locker, he/she sees lockers denoted by the names of offerors. When the user opens such a locker X of an offeror (by clicking on the icon in the display of his/her client program), the server searches the provisioning lockers of the offeror for user lockers that were set up by the offeror for the user, and selects therefrom the user lockers that the user is allowed to access under the current session data. The server sends these names to the client program, which displays them as sub-lockers of X. Thus, the user lockers are not actually contained in X, which, however, is not noticeable by the user.

[0033] The references offered (offered files are visible to the user) are reported by the server to the client program only if the conditions specified in the reference are not violated by any session datum.

[0034] From the description, it becomes clear that a user sees a reference in his/her client program only if the reference contains an encrypted access key that is encrypted with the public key of the user. Using his/her secret key and the encrypted access key, the user can restore the access key of the file and decrypt the encrypted data.

Owner:					
Creation date:					
Right to "enter" co-user 1:	location a ... location z	time a ... time z	auth a ... auth z		
Right to "enter" co-user n:	"	"	"		
Upper limits:	individual file size	total file size	number of sub-lockers		
Limitations:	file type				

Table 1: special folder file

Definition:	system-created file; representative of a file in the system locker	
Data fields:	identifier of the referenced file; encrypted encryption key; type of file; size of file; file creation time; reference creation time; time of last access.	
Security information:	owner; restriction authentication	

Table 2: reference